Практическая работа

Построение модели угроз безопасности персональных данных

Разработка модели угроз безопасности персональных данных при их обработке в ИСПДн осуществляется на основании сведений, полученных на этапе обследования, отдельно для каждой ИСПДн. Модель угроз подготавливается в соответствии с методическими документами ФСТЭК России и включает перечень угроз безопасности персональных данных (УБПДн) с оценкой их актуальности для конкретного оператора.

Моделирование угроз осуществляется экспертным методом. Это значит, что разрабатывать модель угроз должно лицо, имеющее соответствующее образование в сфере защиты информации. Неправильное моделирование угроз неизбежно приводит к увеличению рисков возникновения инцидентов информационной безопасности, созданию предпосылок к нарушению прав субъектов персональных данных, репутационным и материальным потерям оператора.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных разработана ФСТЭК России с учетом действующих нормативных документов ФСТЭК России по защите информации.

В соответствии со статьей 19 Федерального закона «О персональных данных» персональные данные должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. УБПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных

сообществ, отдельных организаций и граждан, а также иными источниками угроз.

УБПДн могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой персональных данных по техническим каналам, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Выявление технических каналов утечки персональных данных осуществляется на основе нормативных и методических документов ФСТЭК России.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации.

Для ИСПДн в общем случае можно выделить следующие угрозы:

1. Угрозы утечки по техническим каналам.
   1.1. Угрозы утечки акустической информации.
   1.2. Угрозы утечки видовой информации.
   1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации.
   2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.
      2.1.1. Кража ПЭВМ;

2.1.2. Кража носителей информации;

2.1.3. Кража ключей и атрибутов доступа;

2.1.4. Кражи, модификации, уничтожения информации;

2.1.5. Вывод из строя узлов ПЭВМ, каналов связи;

2.1.6. Несанкционированное отключение средств защиты.

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

2.2.1. Действия вредоносных программ (вирусов);

2.2.2. Недекларированные возможности системного программного обеспечения (ПО) и ПО для обработки персональных данных;

2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей.

2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

2.3.1. Утрата ключей и атрибутов доступа;

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками;

2.3.3. Непреднамеренное отключение средств защиты;

2.3.4. Выход из строя аппаратно-программных средств;

2.3.5. Сбой системы электроснабжения;

2.3.6. Стихийное бедствие.

2.4. Угрозы преднамеренных действий внутренних нарушителей.

2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

2.5. Угрозы несанкционированного доступа по каналам связи.

2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

2.5.1.1. Перехват за переделами с контролируемой зоны;

2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;

2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.

2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

2.5.3. Угрозы выявления паролей по сети.

2.5.4. Угрозы навязывание ложного маршрута сети.

2.5.5. Угрозы подмены доверенного объекта в сети.

2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

2.5.7. Угрозы типа «Отказ в обслуживании».

2.5.8. Угрозы удаленного запуска приложений.

2.5.9. Угрозы внедрения по сети вредоносных программ.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под **уровнем исходной защищенности ИСПДн** понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 2.1.

Таблица 2.1. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации		+	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		+	
локальная ИСПДн, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			+
ИСПДн, имеющая одноточечный выход в сеть общего пользования		+	
ИСПДн, физически отделенная от сети общего пользования	+		
3. По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск	+		
запись, удаление, сортировка		+	
модификация, передача			+
4. По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные переченем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн		+	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн			+
ИСПДн с открытым доступом			+
5. По наличию соединений с другими базами ПДн иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			+
ИСПДн, в которой используется	+		

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			
6. По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	+		
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации		+	
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с ПДн			+
ИСПДн, предоставляющая часть ПДн		+	
ИСПДн, не предоставляющая никакой информации	+		

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет **высокий уровень исходной защищенности**, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет **средний уровень исходной защищенности**, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет **низкую степень исходной защищенности**, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент $\mathbf{Y_1}$, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под **частотой (вероятностью) реализации угрозы** понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент $\mathbf{Y_2}$, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$\mathbf{Y = (Y_1 + Y_2) / 20}$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признается **низкой**;

если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается **средней**;

если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признается **высокой**;

если $\mathbf{Y > 0{,}8}$, то возможность реализации угрозы признается **очень высокой**.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 2.2.

Таблица 2.2. Правила отнесения угрозы безопасности персональных данных к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

С использованием данных об уровне защищенности ИСПДн и составленного перечня актуальных угроз формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Задание

На основе исходных данных, предоставленных преподавателем, и описанной методики определения актуальных УБПДн построить модель УБПДн.

Отчет о практической работе должен содержать описание процесса построения модели УБПДн, перечень актуальных УБПДн и их описание (последствия реализации).